What is Claimed Is:

1. A method in a unified communications system, the method comprising:

receiving a request for a user interface session to enable a user to leave a message for an identified destination subscriber;

generating a first prompt enabling the user to select encryption of the message;

generating a second prompt, based on the user selecting encryption of the message, for the user to supply an encryption key;

causing encryption of the message into an encrypted message based on the encryption key supplied by the user; and

outputting the encrypted message to a determined destination based on determined subscriber profile attributes for the identified destination subscriber.

2. The method of claim 1, wherein the causing encryption step includes invoking a prescribed encryption utility for generation of the encrypted message.

3. The method of claim 1, further comprising receiving a message data file having the message and a Multipurpose Internet Mail Extension (MIME) that specifies a format of the message, the causing encryption step including encrypting the message data file into an encrypted file having a MIME extension specifying that the encrypted file has an encrypted format.

4. The method of claim 3, wherein the causing encryption step further including generating a message transport header specifying an IP based destination address corresponding to the identified destination subscriber.

5. The method of claim 3, wherein the message data file has a MIME extension specifying a .wav format, the message having an audio header and audio payload, the causing encryption step including encrypting the audio header and the audio payload within the

encrypted file.

6. The method of claim 1, further comprising determining the subscriber profile attributes for the identified destination subscriber based on accessing a subscriber directory according to Lightweight Directory Access Protocol (LDAP), the subscriber profile attributes specifying the determined destination.

7. The method of claim 1, wherein the outputting step includes outputting the encrypted message to the determined destination according to at least one of SMTP protocol and IMAP protocol.

8. The method of claim 1, further comprising:

receiving a request for a second user interface session to enable the identified destination subscriber to retrieve stored messages;

retrieving information related to the stored messages for the identified destination subscriber;

detecting one of the stored messages as encrypted;

generating a third prompt, based on detecting the one stored message, for the identified destination subscriber to supply a decryption key; and

supplying the decryption key and the one stored message to an invoked decryption utility for decryption of the one stored message into a decrypted data file.

9. The method of claim 8, further comprising outputting the decrypted data file during the second user interface session to the identified destination subscriber, independent of the encryption key matching the decryption key.

10. The method of claim 1, wherein the receiving step includes receiving the request according to hypertext transport protocol.

11. A method in a unified communications system, the method comprising:

receiving a request for a user interface session to enable a messaging subscriber to retrieve stored messages;

accessing subscriber profile information from a subscriber profile directory according to a prescribed open network protocol;

determining one of the stored messages is encrypted based on access of a message store according to a prescribed open network protocol and based on the accessed subscriber profile information;

generating a prompt, based on identifying the one stored message as encrypted, for the messaging subscriber to supply a decryption key; and

attempting decrypting of the one stored message based on the decryption key supplied by the messaging subscriber.

12. The method of claim 11, further comprising:

obtaining a decryption result based on the attempting decrypting step; and

outputting the decryption result for attempted presentation to the messaging subscriber.

13. The method of claim 12, wherein the outputting step includes outputting the decryption result independent of whether the decryption key enabled successful decryption of the one stored message.

14. The method of claim 11, wherein the attempting decrypting step includes invoking a prescribed decryption utility for generation of the decryption result based on the decryption key.

15. The method of claim 11, further comprising obtaining, based on the attempting decrypting step, a decryption result including a message data file having a message and a Multipurpose Internet Mail Extension (MIME) that specifies a format of the message.

16. The method of claim 11, wherein the receiving step includes receiving the request according to hypertext transport protocol.

17. The method of claim 11, wherein the accessing step includes obtaining the subscriber profile information according to LDAP protocol.

18. The method of claim 17, wherein the determining step includes:

accessing the message store according to IMAP protocol for messaging information related to the stored messages for the messaging subscriber, based on the accessed subscriber profile information; and

identifying the one stored message as encrypted based on a prescribed file extension specifying that the one stored message has an encrypted format.

19. The method of claim 18, wherein the identifying step includes identifying the prescribed file extension as a MIME type extension that specifies an encrypted format.

20. The method of claim 11, wherein the determining step includes:

accessing the message store according to IMAP protocol for messaging information related to the stored messages for the messaging subscriber, based on the accessed subscriber profile information; and

identifying the one stored message as encrypted based on a prescribed file extension specifying that the one stored message has an encrypted format.

21. The method of claim 20, wherein the identifying step includes identifying the prescribed file extension as a MIME type extension that specifies an encrypted format.

22. A unified communications server including:

an interface configured for receiving a request for a user interface session to enable a user to leave a message for an identified destination subscriber;

an IP-based interface enabling retrieval of subscriber profile attributes for the identified destination subscriber from an IP-based subscriber profile directory, and storage of messaging information for the identified destination subscriber in an IP-based subscriber message store; and

an application runtime environment configured for generating the user interface session and accessing the subscriber profile attributes, the application runtime environment configured for generating first and second prompts enabling the user to select encryption of the message and input an encryption key, respectively, the application runtime environment configured for causing the message to be encrypted into an encrypted file based on the encryption key supplied by the user, and outputting an encrypted message including the encrypted file for storage in the IP-based subscriber message store for the identified destination subscriber.

23. The server of claim 22, wherein the application runtime environment is configured for invoking a prescribed encryption utility for generation of the encrypted file.

24. The server of claim 23, wherein the application runtime environment is configured for generating for the encrypted message a MIME extension specifying that the encrypted file has an encrypted format, and a message transport header specifying an IP based destination address corresponding to the identified destination subscriber.

25. The server of claim 22, further comprising an application programming interface configured for invoking prescribed routines, including a first routine for accessing the IP-based subscriber profile directory according to LDAP protocol, and a second routine for accessing the IP-based subscriber message store according to at least one of SMTP protocol and IMAP protocol.

26. The server of claim 25, wherein the application programming interface is configured for invoking a prescribed encryption utility for generation of the encrypted message.

27. The server of claim 22, wherein the application runtime environment is further configured for generating a second user interface session enabling the identified destination subscriber to retrieve stored messages, the application runtime environment, in response to detecting one of the stored messages as encrypted, generating a third prompt for the identified destination subscriber to supply a decryption key, the application runtime environment causing attempted decryption of the one stored message based on the decryption key supplied by the user.

28. The server of claim 27, wherein the application runtime environment, upon obtaining a decryption result based on the attempted decryption, outputs the decryption result for attempted presentation to the identified destination subscriber independent of whether the decryption key enabled successful decryption of the one stored message.

29. The server of claim 22, wherein the interface is configured for receiving the request, and outputting responses, according to hypertext transport protocol.

30. A unified communications server comprising:

an interface configured for receiving a request for a user interface session to enable a messaging subscriber to retrieve stored messages;

an IP-based interface enabling retrieval of subscriber profile attributes for the messaging subscriber from an IP-based subscriber profile directory, and access of messaging information for the messaging subscriber from an IP-based subscriber message store; and

an application runtime environment configured for generating the user interface session and accessing the subscriber profile attributes, the application runtime environment configured for generating, based on identifying from the messaging information that one of the stored messages is encrypted, a prompt for the messaging subscriber to supply a decryption key, the application runtime environment causing attempted decryption of the one stored message into a decryption result based on the decryption key supplied by the user.

31. The server of claim 30, wherein the application runtime environment is configured for invoking a prescribed decryption utility for the attempted decryption of the one stored message into the decryption result.

32. The server of claim 31, wherein the application runtime environment is configured for outputting the decryption result to the messaging subscriber independent of whether the decryption key enabled successful decryption of the one stored message.

33. The server of claim 30, wherein the application runtime environment identifies that the one stored message is encrypted based on an attached MIME extension specifying an encrypted format.

34. The server of claim 30, further comprising an application programming interface configured for invoking prescribed routines, including a first routine for accessing the IP-based subscriber profile directory according to LDAP protocol, and a second routine for accessing the IP-based subscriber message store according to IMAP protocol.

35. The server of claim 34, wherein the application programming interface is configured for invoking a prescribed decryption utility for generation of the decryption result.

36. The server of claim 30, the interface is configured for receiving the request, and outputting responses, according to hypertext transport protocol.

37. A computer readable medium having stored thereon sequences of instructions for receiving a message for an identified messaging subscriber, the sequences of instructions including instructions for performing the steps of:

receiving a request for a user interface session to enable a user to leave a message for an identified destination subscriber;

generating a first prompt enabling the user to select encryption of the message;

generating a second prompt, based on the user selecting encryption of the message, for the user to supply an encryption key;

causing encryption of the message into an encrypted message based on the encryption key supplied by the user; and

outputting the encrypted message to a determined destination based on determined subscriber profile attributes for the identified destination subscriber.

38. The medium of claim 37, wherein the causing encryption step includes invoking a prescribed encryption utility for generation of the encrypted message.

39. The medium of claim 37, further comprising instructions for performing the step of receiving a message data file having the message and a Multipurpose Internet Mail Extension (MIME) that specifies a format of the message, the causing encryption step including encrypting the message data file into an encrypted file having a MIME extension specifying that the encrypted file has an encrypted format.

40. The medium of claim 39, wherein the causing encryption step further including generating a message transport header specifying an IP based destination address corresponding to the identified destination subscriber.

41. The medium of claim 39, wherein the message data file has a MIME extension specifying a .wav format, the message having an audio header and audio payload, the causing encryption step including encrypting the audio header and the audio payload within the encrypted file.

42. The medium of claim 37, further comprising instructions for performing the step of determining the subscriber profile attributes for the identified destination subscriber based on accessing a subscriber directory according to Lightweight Directory Access Protocol (LDAP), the subscriber profile attributes specifying the determined destination.

43. The medium of claim 37, wherein the outputting step includes outputting the encrypted message to the determined destination according to at least one of SMTP protocol and IMAP protocol.

44. The medium of claim 37, further comprising instructions for performing the steps of:

receiving a request for a second user interface session to enable the identified destination subscriber to retrieve stored messages;

retrieving information related to the stored messages for the identified destination subscriber;

detecting one of the stored messages as encrypted;

generating a third prompt, based on detecting the one stored message, for the identified destination subscriber to supply a decryption key; and

supplying the decryption key and the one stored message to an invoked decryption utility for decryption of the one stored message into a decrypted data file.

45. The medium of claim 44, further comprising instructions for performing the step of outputting the decrypted data file during the second user interface session to the identified destination subscriber, independent of the encryption key matching the decryption key.

46. The medium of claim 37, wherein the receiving step includes receiving the request according to hypertext transport protocol.

47. A computer readable medium having stored thereon sequences of instructions for retrieving a message for a messaging subscriber, the sequences of instructions including instructions for performing the steps of::

receiving a request for a user interface session to enable a messaging subscriber to retrieve stored messages;

accessing subscriber profile information from a subscriber profile directory according to a prescribed open network protocol;

determining one of the stored messages is encrypted based on access of a message store according to a prescribed open network protocol and based on the accessed subscriber profile information;

generating a prompt, based on identifying the one stored message as encrypted, for the messaging subscriber to supply a decryption key; and

attempting decrypting of the one stored message based on the decryption key supplied by the messaging subscriber.

48. The medium of claim 47, further comprising instructions for performing the steps of:

obtaining a decryption result based on the attempting decrypting step; and

outputting the decryption result for attempted presentation to the messaging subscriber.

49. The medium of claim 48, wherein the outputting step includes outputting the decryption result independent of whether the decryption key enabled successful decryption of the one stored message.

50. The medium of claim 47, wherein the attempting decrypting step includes invoking a prescribed decryption utility for generation of the decryption result based on the decryption key.

51. The medium of claim 47, further comprising instructions for performing the step of obtaining, based on the attempting decrypting step, a decryption result including a message data file having a message and a Multipurpose Internet Mail Extension (MIME) that specifies a format of the message.

52. The medium of claim 47, wherein the receiving step includes receiving the request according to hypertext transport protocol.

53. The medium of claim 47, wherein the accessing step includes obtaining the subscriber profile information according to LDAP protocol.

54. The medium of claim 53, wherein the determining step includes:

accessing the message store according to IMAP protocol for messaging information related to the stored messages for the messaging subscriber, based on the accessed subscriber profile information; and

identifying the one stored message as encrypted based on a prescribed file extension specifying that the one stored message has an encrypted format.

55. The medium of claim 54, wherein the identifying step includes identifying the prescribed file extension as a MIME type extension that specifies an encrypted format.

56. The medium of claim 47, wherein the determining step includes:

accessing the message store according to IMAP protocol for messaging information related to the stored messages for the messaging subscriber, based on the accessed subscriber profile information; and

identifying the one stored message as encrypted based on a prescribed file extension specifying that the one stored message has an encrypted format.

57. The medium of claim 56, wherein the identifying step includes identifying the prescribed file extension as a MIME type extension that specifies an encrypted format.

58. A unified communications system comprising:

means for receiving a request for a user interface session to enable a user to leave a message for an identified destination subscriber;

means for generating a first prompt enabling the user to select encryption of the message;

means for generating a second prompt, based on the user selecting encryption of the message, for the user to supply an encryption key;

means for causing encryption of the message into an encrypted message based on the encryption key supplied by the user; and

means for outputting the encrypted message to a determined destination based on determined subscriber profile attributes for the identified destination subscriber.

59. The system of claim 58, wherein the causing encryption means is configured for invoking a prescribed encryption utility for generation of the encrypted message.

60. The system of claim 58, further comprising means for receiving a message data file having the message and a Multipurpose Internet Mail Extension (MIME) that specifies a format of the message, the causing encryption means configured for causing encryption of the message data file into an encrypted file having a MIME extension specifying that the encrypted file has an encrypted format.

61. The system of claim 60, wherein the causing encryption means is configured for generating a message transport header specifying an IP based destination address corresponding to the identified destination subscriber.

62. The system of claim 60, wherein the message data file has a MIME extension specifying a .wav format, the message having an audio header and audio payload, the causing encryption means causing the audio header and the audio payload to be encrypted within the encrypted file.

63. The system of claim 58, further comprising means for determining the subscriber profile attributes for the identified destination subscriber based on accessing a subscriber directory according to Lightweight Directory Access Protocol (LDAP), the subscriber profile attributes specifying the determined destination.

64. The system of claim 58, wherein the outputting means is configured for outputting the encrypted message to the determined destination according to at least one of SMTP protocol and IMAP protocol.

65. The system of claim 58, wherein the receiving means also is configured for receiving a request for a second user interface session to enable the identified destination subscriber to retrieve stored messages, the system further comprising:

means for retrieving information related to the stored messages for the identified destination subscriber;

means for detecting one of the stored messages as encrypted;

means for generating a third prompt, based on detecting the one stored message, for the identified destination subscriber to supply a decryption key; and

means for supplying the decryption key and the one stored message to an invoked decryption utility for decryption of the one stored message into a decrypted data file.

66. The system of claim 65, further comprising means for outputting the decrypted data file during the second user interface session to the identified destination subscriber, independent of the encryption key matching the decryption key.

67. The system of claim 58, wherein the receiving means is configured for receiving the request according to hypertext transport protocol.

68. A unified communications system comprising:

means for receiving a request for a user interface session to enable a messaging subscriber to retrieve stored messages;

means for accessing subscriber profile information from a subscriber profile directory according to a prescribed open network protocol;

means for determining one of the stored messages is encrypted based on access of a message store according to a prescribed open network protocol and based on the accessed subscriber profile information;

means for generating a prompt, based on identifying the one stored message as encrypted, for the messaging subscriber to supply a decryption key; and

means for attempting decrypting of the one stored message based on the decryption key supplied by the messaging subscriber.

69. The system of claim 68, further comprising:

means for obtaining a decryption result based on the attempting decrypting step; and

means for outputting the decryption result for attempted presentation to the messaging subscriber.

70. The system of claim 69, wherein the outputting means is configured for outputting the decryption result independent of whether the decryption key enabled successful decryption of the one stored message.

71. The system of claim 68, wherein the attempting decrypting means is configured for invoking a prescribed decryption utility for generation of the decryption result based on the decryption key.

72. The system of claim 68, wherein the attempting decrypting means obtains a decryption result including a message data file having a message and a Multipurpose Internet Mail Extension (MIME) that specifies a format of the message.

73. The system of claim 68, wherein the receiving means is configured for receiving the request according to hypertext transport protocol.

74. The system of claim 68, wherein the accessing means is configured for obtaining the subscriber profile information according to LDAP protocol.

75. The system of claim 74, wherein the determining means is configured for:

accessing the message store according to IMAP protocol for messaging information related to the stored messages for the messaging subscriber, based on the accessed subscriber profile information; and

identifying the one stored message as encrypted based on a prescribed file extension specifying that the one stored message has an encrypted format.

76. The system of claim 75, wherein the determining means identifies the prescribed file extension as a MIME type extension that specifies an encrypted format.

77. The system of claim 68, wherein the determining means is configured for:

accessing the message store according to IMAP protocol for messaging information related to the stored messages for the messaging subscriber, based on the accessed subscriber profile information; and

identifying the one stored message as encrypted based on a prescribed file extension specifying that the one stored message has an encrypted format.

78. The system of claim 77, wherein the determining means is configured for identifying the prescribed file extension as a MIME type extension that specifies an encrypted format.